IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Withdrawn): An information furnishing medium connected over a network to a pre-set information processing apparatus, comprising:

communication means for receiving a pre-set program from said information processing apparatus and for transmitting said program in an encrypted form to said information processing apparatus; and

encrypting means for encrypting said program received by said communication means.

Claim 2 (Withdrawn): The information processing apparatus according to claim 1 wherein said program is a source program executed by an interpreter.

Claim 3 (Withdrawn): The information processing apparatus according to claim 1 wherein said program is an object program.

Claim 4 (Withdrawn): A method for furnishing the information by an information furnishing medium connected over a network to sa pre-set information processing apparatus, comprising:

a communication step of receiving a pre-set program from said information processing apparatus and for transmitting said program in an encrypted form to said information processing apparatus; and

an encrypting step of encrypting said program received by said communication step.

Claim 5 (Withdrawn): A furnishing medium for furnishing a computer-readable

program for executing the processing comprising:

a communication step of receiving a pre-set program from said information

processing apparatus and for transmitting said program in an encrypted form to said

·information processing apparatus; and

an encrypting step of encrypting said program received by said communication step.

Claim 6 (Currently Amended): An information processing apparatus for reciprocal

authentication with another information processing apparatus to execute pre-set processing,

comprising:

receiving means for receiving a key category, a random number, and a device ID from

said another information processing apparatus;

selection means for selecting the processing for reciprocal authentication being

executed from one or more reciprocal authentication procedures in keeping with said pre-set

processing;

reciprocal authentication means for executing the selected reciprocal authentication

procedures by said selection means based on the key category; and

key creation means for establishing a common key shared with said another

information processing apparatus based on the key category and device ID.

Claim 7 (Currently Amended): A method for processing the information by an

information processing apparatus for reciprocal authentication with another information

processing apparatus to execute pre-set processing, said method comprising:

receiving a key category, a random umber, and a device ID from said another

information processing apparatus;

selecting the processing for reciprocal authentication being executed from one or

more reciprocal authentication procedures in keeping with said pre-set processing;

executing the selected reciprocal authentication procedures by said selection means;

and

establishing a common key shared with said another information processing apparatus

based on the key category and device ID.

Claim 8 (Currently Amended): A furnishing medium for furnishing a computer-

readable program for executing the processing comprising:

receiving a key category, a random number, and a device ID from said another

information processing apparatus;

selecting the processing for reciprocal authentication being executed from one or

more reciprocal authentication procedures in keeping with said pre-set processing;

executing the selected reciprocal authentication procedures by said selection means;

and

establishing a common key shared with said another information processing apparatus

based on the key category and device ID.

Claim 9 (Withdrawn): A method for authentication comprising:

generating a first random number in a first apparatus;

transmitting an ID, the key attribute information and said first random number of said

first apparatus from said first apparatus to a second apparatus;

generating a second random number in said second apparatus;

receiving the ID, key attribute information and the first random number of the first apparatus, transmitted from said first apparatus, by said second apparatus;

computing the key in said second apparatus from the key attribute information;

generating a third random number from said key and the first and second random numbers in said second apparatus;

transmitting the information on the second and third random numbers and the key from said second apparatus to said first apparatus;

receiving the information on the second and third random numbers and the key transmitted from said second apparatus in said first apparatus;

generating the key from said information on the key in said first apparatus;

generating a fourth random number from said key and the first and second random numbers in said first apparatus;

transmitting said fourth random number from said first apparatus to said second apparatus; and

finding a transient key from the third and fourth random number and the key in each of the first and second apparatus.

Claim 10 (Withdrawn): A method for authentication comprising:

generating a first random number in a first apparatus;

transmitting an ID of the first apparatus, the key attribute information of said first apparatus, the key attribute information of a second apparatus and said first random number from said first apparatus to said second apparatus;

generating a second random number in said second apparatus;

receiving the ID of said first apparatus, key attribute information of said first

apparatus, key attribute information of said second apparatus and said first random number,

transmitted from said first apparatus, in said second apparatus;

computing a first key in said second apparatus from the key attribute information of

said second apparatus;

computing a second key in said second apparatus from the key attribute information

of said first apparatus;

generating a third random number from said key and the first and second random

numbers in said second apparatus;

transmitting the information on the second and third random numbers and the key

from said second apparatus to said first apparatus;

receiving the information on the second and third random numbers and the key

transmitted from said second apparatus in said first apparatus;

generating a second key from said information on the key in said first apparatus;

generating a fourth random number from said key and the first and second random

numbers in said first apparatus;

transmitting said fourth random number from said first apparatus to said second

apparatus; and

finding a transient key from the third and fourth random number and the second key

in each of the first and second apparatus.

Claims 11-14 (Canceled).

Claim 15 (Withdrawn): An information processing apparatus comprising:

first execution means for decoding and executing an encrypted program; and

second execution means for furnishing said program to said first execution means,

decoding the encrypted program and for executing said program based on the results of

execution of said first execution means.

Claim 16 (Withdrawn): The information processing apparatus according to claim 1

wherein said first and second execution means are provided on respective independent

hardwares.

Claim 17 (Withdrawn): The information processing apparatus according to claim 15

wherein said program is a source program executed by an interpreter.

Claim 18 (Withdrawn): The information processing apparatus according to claim 15

wherein said program is an object program.

Claim 19 (Withdrawn): A method for processing the information of an information

processing apparatus comprising:

a first execution step of decoding and executing an encrypted program; and

a second execution step of furnishing said program to said first execution step,

decoding the encrypted program and for executing said program based on the results of

execution of said first execution step.

Application No. 09/701,084   Atty. Docket No. 204478US-6PCT

Reply to Office Action of November 29, 2005

Claim 20 (Withdrawn): A furnishing medium for furnishing a computer-readable program executing the processing comprising:

a first execution step of decoding and executing an encrypted program; and

a second execution step of furnishing said program to said first execution step, decoding the encrypted program and for executing said program based on the results of execution of said first execution step.

Claim 21 (Withdrawn): An information processing apparatus having a semiconductor IC loaded thereon and adapted for furnishing a program to be executed by said semiconductor IC, said apparatus comprising:

communication means for transmitting said program for execution by said semiconductor IC to an authentication station and for receiving the encrypted program from said authentication station;

recording means for recording the encrypted program received from said authentication station; and

transmitting means for transmitting said program recorded on said recording means to said semiconductor IC.

Claim 22 (Withdrawn): The information processing apparatus according to claim 20 wherein said program is a source program for execution by an interpreter.

Claim 23 (Withdrawn): The information processing apparatus according to claim 20 wherein said program is an object program.

Claim 24 (Withdrawn): An information processing method for an information

processing apparatus having a semiconductor IC loaded thereon and adapted for furnishing a

program to be executed by said semiconductor IC, said apparatus comprising:

a communication step of transmitting said program for execution by said

semiconductor IC to an authentication station and for receiving the encrypted program from

said authentication station;

a recording step of recording the encrypted program received from said authentication

station; and

a transmitting step of transmitting said program recorded on said recording means to

said semiconductor IC.

Claim 25 (Withdrawn): A furnishing medium for furnishing a computer-readable

program adapted for causing execution of a processing by an information processing

apparatus having a semiconductor IC loaded thereon and adapted for furnishing a program to

be executed by said semiconductor IC, said processing comprising:

a communication step of transmitting said program for execution by said

semiconductor IC to an authentication station and for receiving the encrypted program from

said authentication station;

a recording step of recording the encrypted program received from said authentication

station; and

a transmitting step of transmitting said program recorded on said recording means to

said semiconductor IC.

Claim 26 (Withdrawn): An information processing system comprising:

an information processing apparatus having a semiconductor IC loaded thereon and

adapted for furnishing a program to be executed by said semiconductor IC; and

an authentication station;

said information processing apparatus including

communication means for transmitting said program for execution by said

semiconductor IC to said authentication station and for receiving the encrypted program from

said authentication station;

recording means for recording the encrypted program received from said

authentication station; and

transmitting means for transmitting said program recorded on said recording means to

said semiconductor IC;

said authentication station including

communication means for receiving said program executed by said semiconductor IC

and for transmitting the encrypted program to said information processing apparatus; and

encryption means for encrypting said program, received by said communication

means, in a pre-set system.

Claim 27 (Withdrawn): An information processing apparatus having a

semiconductor IC loaded thereon and adapted for furnishing a program to be executed by said

semiconductor IC, said apparatus comprising:

re-arraying means for re-arraying commands of a command queue contained in said

program executed by said semiconductor IC;

recording means for recording said program in which said command queue has been

re-arrayed; and

transmission means for transmitting said program recorded on said recording means

to said semiconductor IC.

Claim 28 (Withdrawn): The information processing apparatus according to claim 26

wherein said program is a source program for execution by an interpreter.

Claim 29 (Withdrawn): The information processing apparatus according to claim 26

wherein said program is an object program.

Claim 30 (Withdrawn): An information processing method for an information

processing apparatus having a semiconductor IC loaded thereon and adapted for furnishing a

program to be executed by said semiconductor IC, said method comprising:

a re-arraying step of re-arraying commands of a command queue contained in said

program executed by said semiconductor IC;

a recording step of recording said program in which said command queue has been re-

arrayed; and

a transmission step of transmitting said program recorded on said recording means to

said semiconductor IC.

Claim 31 (Withdrawn): A furnishing medium for furnishing a computer-readable

program adapted for causing execution of a processing by an information processing

apparatus having a semiconductor IC loaded thereon and adapted for furnishing a program to

be executed by said semiconductor IC, said processing comprising:

a re-arraying step of re-arraying commands of a command queue contained in said

program executed by said semiconductor IC;

a recording step of recording said program in which said command queue has been re-

arrayed; and

a transmission step of transmitting said program recorded on said recording means to

said semiconductor IC.

Claim 32 (Withdrawn): An information processing apparatus having a

semiconductor IC loaded thereon and adapted for furnishing a program to be executed by said

semiconductor IC, said apparatus comprising:

re-arraying means for re-arraying commands of a command queue contained in said

program executed by said semiconductor IC;

encrypting means for encrypting said program;

recording means for recording said program which has been encrypted and in which

said command queue has been re-arrayed; and

transmission means for transmitting said program recorded on said recording means

to said semiconductor IC.

Claim 33 (Withdrawn): The information processing apparatus according to claim 31

wherein said program is a source program for execution by an interpreter.

Claim 34 (Withdrawn): The information processing apparatus according to claim 31 wherein said program is an object program.

Claim 35 (Withdrawn): An information processing method for an information processing apparatus having a semiconductor IC loaded thereon and adapted for furnishing a program to be executed by said semiconductor IC, said method comprising:

a re-arraying step of re-arraying commands of a command queue contained in said program executed by said semiconductor IC;

an encrypting step of encrypting said program;

a recording step of recording said program which has been encrypted and in which said command queue has been re-arrayed; and

a transmission step of transmitting said program recorded on said recording means to said semiconductor IC.

Claim 36 (Withdrawn): A furnishing medium for furnishing a computer-readable program adapted for causing execution of a processing by an information processing apparatus having a semiconductor IC loaded thereon and adapted for furnishing a program to be executed by said semiconductor IC, said processing comprising:

a re-arraying step of re-arraying commands of a command queue contained in said program executed by said semiconductor IC;

an encrypting step of encrypting said program;

a recording step of recording said program which has been encrypted and in which said command queue has been re-arrayed; and

a transmission step of transmitting said program recorded on said recording means to
said semiconductor IC.

Claim 37 (Withdrawn): A semiconductor IC loaded on an information processing
apparatus and adapted for executing variable processing based on commands from said
information processing apparatus, comprising:

reception means for receiving an encrypted first program transmitted from said
information processing apparatus;

decoding means for decoding said first program received by said reception means;

holding means for holding a second program adapted for processing the first program
decoded by said decoding means;

executing means for executing said first program processed based on said second
program held by said holding means;

transmitting means for transmitting the results of execution by said execution means
to said information processing apparatus; and

time-keeping means for performing the time-keeping operation and for correcting the
current time based on the time information from said information processing apparatus.

Claim 38 (Withdrawn): The semiconductor IC according to claim 36 further
comprising:

non-volatile memory means for storing data used by said information processing
apparatus.

Claim 39 (Withdrawn): A method for processing the information of a semiconductor IC loaded on an information processing apparatus and adapted for executing variable processing operations based on commands from said information processing apparatus, comprising:

a reception step of receiving an encrypted first program transmitted from said information processing apparatus;

a decoding step of decoding said first program received by said reception step;

a holding step of holding a second program adapted for processing the first program decoded by said decoding step;

an executing step of executing said first program processed based on said second program held by said holding step;

a transmitting step of transmitting the results of execution by said execution step to said information processing apparatus; and

a time-keeping step of performing the time-keeping operation and for correcting the current time based on the time information from said information processing apparatus.

Claim 40 (Withdrawn): A furnishing medium for furnishing a computer-readable program for causing execution of a processing by a semiconductor IC loaded on an information processing apparatus and adapted for executing variable processing based on commands from said information processing apparatus, said processing including

a reception step of receiving an encrypted first program transmitted from said information processing apparatus;

a decoding step of decoding said first program received by said reception step;

a holding step of holding a second program adapted for processing the first program

decoded by said decoding step;

an executing step of executing said first program processed based on said second

program held by said holding step;

a transmitting step of transmitting the results of execution by said execution step to

said information processing apparatus; and

a time-keeping step of performing the time-keeping operation and for correcting the

current time based on the time information from said information processing apparatus.

Claim 41 (Withdrawn): An information processing apparatus for outputting variable

commands to a loaded semiconductor IC for execution thereby, said apparatus comprising:

transmission means for transmitting an encrypted program to said semiconductor IC;

first reception means for receiving output data which is the result of processing of said

program by said semiconductor IC;

second reception means for receiving data and the time information from another

apparatus;

storage means for storing data received by said second reception means; and

correction means for correcting the time information of said semiconductor IC based

on the time information received by said second reception means.

Claim 42 (Withdrawn): An information processing method for an information

processing apparatus adapted for outputting variable commands to a loaded semiconductor IC

for execution thereby, said method comprising:

a transmission step of transmitting an encrypted program to said semiconductor IC;

a first reception step of receiving output data which is the result of processing of said

program by said semiconductor IC;

a second reception step of receiving data and the time information from another

apparatus;

a storage step of storing data received by said second reception step; and

a correction step of correcting the time information of said semiconductor IC based on

the time information received by said second reception step.

Claim 43 (Withdrawn): A furnishing medium for furnishing a computer-readable

program for causing an information processing apparatus to execute a processing, said

information processing apparatus being adapted to output variable commands to a

semiconductor IC loaded thereon for execution thereby, said processing including

a transmission step of transmitting an encrypted program to said semiconductor IC;

a first reception step of receiving output data which is the result of processing of said

program by said semiconductor IC;

a second reception step of receiving data and the time information from another

apparatus;

a storage step of storing data received by said second reception step; and

a correction step of correcting the time information of said semiconductor IC based on

the time information received by said second reception step.

Claim 44 (Withdrawn): An information processing apparatus for outputting variable

commands to a loaded semiconductor IC for execution thereby, said apparatus comprising:

storage means for storing said program and data required for executing the program;

control means for controlling storage or readout of said program and the data for said

storage means;

first encryption means for encrypting said program with a first key supplied from said

semiconductor IC; and

second encryption means for encrypting said data with a second key supplied from

said semiconductor IC.

Claim 45 (Withdrawn): The information processing apparatus according to claim 43

wherein said first key is determined by attributes of said program.

Claim 46 (Withdrawn): The information processing apparatus according to claim 43

wherein said second key is determined by attributes of said program and a third key

previously stored by said semiconductor IC.

Claim 47 (Withdrawn): An information processing method for an information

processing apparatus adapted for outputting variable commands to a loaded semiconductor IC

for execution thereby, said method comprising:

a storage step of storing said program and data required for executing the program;

a control step of controlling storage or readout of said program and the data for said

storage step;

a first encryption step of encrypting said program with a first key supplied from

semiconductor IC; and

a second encryption step of encrypting said data with a second key supplied from said

semiconductor IC.

Claim 48 (Withdrawn): A furnishing medium for furnishing a computer-readable program adapted for causing execution of a processing by an information processing apparatus for outputting variable commands to a loaded semiconductor IC for execution thereby, said processing comprising:

a storage step of storing said program and data required for executing the program;

a control step of controlling storage or readout of said program and the data for said storage step;

a first encryption step of encrypting said program with a first key supplied from said semiconductor IC; and

a second encryption step of encrypting said data with a second key supplied from said semiconductor IC.

Claim 49 (Withdrawn): A semiconductor IC adapted for being loaded on a pre-set information processing apparatus, for receiving a program supplied from the information processing apparatus and data necessary for executing said program, and for executing said program, said semiconductor IC comprising:

storage means for storing a first key proper to said semiconductor IC;

key generating means for generating a second key from said first key stored by said storage means and from the attributes of said program supplied from said information processing apparatus;

first decoding means for decoding said program with a third key; and

second decoding means for decoding said data with said second key.

Claim 50 (Withdrawn): An information processing method for processing the information of a semiconductor IC adapted for being loaded on a pre-set information processing apparatus, for receiving a program supplied from the information processing apparatus and data necessary for executing said program, and for executing said program, said method comprising:

a storage step of storing a first key proper to said semiconductor IC;

a key generating step for generating a second key from said first key stored by said storage step and from the attributes of said program supplied from said information processing apparatus;

a first decoding step of decoding said program with a third key; and

a second decoding step of decoding said data with said second key.

Claim 51 (Withdrawn): A furnishing medium for furnishing a computer-readable program adapted for causing execution of a processing by a semiconductor IC adapted for being loaded on a pre-set information processing apparatus, for receiving a program supplied from the information processing apparatus and data necessary for executing said program, and for executing said program, said processing comprising:

a storage step of storing a first key proper to said semiconductor IC;

a key generating step for generating a second key from said first key stored by said storage step and from the attributes of said program supplied from said information processing apparatus;

a first decoding step of decoding said program with a third key; and

a second decoding step of decoding said data with said second key.

Claim 52 (Withdrawn): An information processing system comprising:

an information processing apparatus for supplying a program executed by said

semiconductor IC and a semiconductor IC adapted for being loaded on a pre-set information

processing apparatus, for receiving a program supplied from the information processing

apparatus and data necessary for executing said program, and for executing said program,

said information processing apparatus including

storage means for storing said program and data required for executing the program;

control means for controlling storage or readout of said program and the data for said

storage means;

first encryption means for encrypting said program with a first key supplied from said

semiconductor IC;

second encryption means for encrypting said data with a second key supplied from

said semiconductor IC; and

first communication means for transmitting the encrypted program and data necessary

for execution of the program to said semiconductor IC and for receiving said first and second

keys from said semiconductor IC;

said semiconductor IC including

second communication means for receiving the encrypted program and data necessary

for executing the program form said information processing apparatus and for transmitting

the first and second keys to said information processing apparatus;

storage means pre-storing a third key proper to said semiconductor IC;

key generating means for generating a second key from said third key stored in said

storage means and from the attribute of the program supplied from said information

processing apparatus;

21

first decoding means for decoding the program received by said second

communication means with a first key; and

second decoding means for decoding said data received by said second

communication means with the second key.

Claim 53 (Currently Amended): An information furnishing medium connected over

a network to a pre-set information processing apparatus, comprising:

receiving unit configured to receive a key category, a random number and device ID

from said another information processing apparatus;

communication unit configured to receive a pre-set program from said information

processing apparatus and for transmitting said program in an encrypted form to said

information processing apparatus;

encrypting unit configured to encrypt said program received by said communication

means; and

key creation unit configured to establish a common key shared with said another

information processing apparatus based on the key category and device ID.

22